Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень Бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: Процедури забезпечення кібергігієни в навчальних закладах

Виконавець: студент IV курсу, групи КБ-41

_____ **Роман ЖОГЛО**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Микола БРАЇЛОВСЬКИЙ	

Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-41** (група) **Роману Юрійовичу Жогло** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Процедури забезпечення кібергігієни в навчальних закладах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Сучасний стан кібергігієни України, кібергігієна закордоном, небезпеки для учнів

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з ситуацією з кібергігієною в Україні, кібербезпекою учнів навчальних закладів, розглянути наявні проблеми груп учнів залежно від віку, сформувати анкету розвитку і рекомендації з кібергігієни для учнів

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації з кібергігієни для учнів навчальних закладів та сформовано анкету розвитку .

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Роман ЖОГЛО
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 29.01.2023	*Виконано*
2	Аналіз літератури	29.01.2023 – 11.02.2023	*Виконано*
3	Обґрунтування вибору напрямку досліджень	12.02.2023 – 15.02.2023	*Виконано*
4	Дослідження стану кібергігієни в суспільстві	16.02.2023 – 04.03.2023	*Виконано*
5	Аналіз проблем загроз учням навчальних закладів	05.03.2023 – 21.03.2023	*Виконано*
6	Синтез та формування анкети розвитку	22.03.2023 – 08.04.2023	*Виконано*
7	Формулювання рекомендацій щодо кібергігієни для учнів навчальних закладів та проведення анкетування	09.04.2023 – 10.05.2023	*Виконано*
8	Оформлення пояснювальної записки	11.05.2023 – 27.05.2023	*Виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2023 – 12.06.2023	*Виконано*

Завдання видав _____ Микола БРАІЛОВСЬКИЙ
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Роман ЖОГЛО
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатку, має 55 сторінок основного тексту, 1 таблицю. Список використаних джерел містить 21 найменування і займає 2 сторінки.

Методи дослідження кваліфікаційної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння проведених раніше досліджень;

Об'єктом дослідження є процес забезпечення кібергігієни в навчальних закладах.

Предметом дослідження в даній роботі є методи, заходи і методики забезпечення процедур кібергігієни в навчальних закладах.

Вивчення та узагальнення вітчизняної і зарубіжної практики. У роботі проаналізована існуюча література з забезпечення процедури кібергігієни навчальних закладів, стан кібергігієни в Україні, потенційні загрози учням навчальних закладів.

Сформована анкета розвитку та рекомендації з кібергігієни для учнів навчальних закладів, розглянуто сильні сторони та обмеження методу анкетування учнів, описано перспективи майбутніх досліджень теми кібергігієни в галузі кібербезпеки.

Ключові слова: кібербезпека, кібергігієна, фішинг, кіберзагрози.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

РФ – Російська Федерація

UISAQ - Анкета інформаційної безпеки користувача;

BCISQ - Анкета біхевіорально-когнітивної безпеки в Інтернеті;

OSBBQ - Анкета поведінки та переконань безпеки в Інтернеті;

HAIS-Q - Анкета людських аспектів інформаційної безпеки;

KAB - Знання, ставлення та поведінка.

K-12 – програма, яка включає в себе державні віртуальні школи, онлайн-школи, які залучають учнів інших країн, і програми, надані окремим школам.

ЗМІСТ

ВСТУП

Кожен навчальний заклад повинен піклуватися про свої дані, а також ризиками використання мережевих комп'ютерів і служб. Саме тому кожен повинен дотримуватися основних принципів кібербезпеки.

Старші керівники повинні знати, що кібербезпека – це питання управління та забезпечення. Після всього, погана кібергігієна може вплинути на здатність школи функціонувати, зберігати свою репутацію та свої юридичні безпечні дані.

Кібербезпека – це захист пристроїв, якими ми всі користуємося і послуги, до яких ми маємо доступ онлайн – як вдома, так і на роботі - від крадіжки або пошкодження.

Це також запобігання несанкціонованому доступу до простору кількість особистої інформації, яку ми зберігаємо на цих пристроях і онлайн.

На сьогоднішній день кібергігієна є дуже важливою темою, оскільки, війна із РФ ведеться не лише за землі України на її територіях, а й в інфопросторі та кіберпросторі.

Раніше Росія використовувала кібератаки проти України для знищення чи пошкодження інфраструктури та даних. 2022 року вона знову спробувала зробити це. Судячи із загальнодоступної інформації, незадовго до вторгнення, РФ розгорнула широку кіберкампанію (список відомих подій див. у додатку). Деякі звіти показали величезне зростання експлойтів першого дня. Зважаючи на все, мета полягала в тому, щоб створити безладдя та розтрощити українську оборону. Росія прагнула порушити роботу сервісів та встановити деструктивне шкідливе програмне забезпечення в українських мережах, включаючи фішинг, відмову в обслуговуванні та використання вразливостей програмного забезпечення. Основними цілями були українські урядові веб-сайти, постачальники енергетичних та телекомунікаційних послуг, фінансові установи та ЗМІ. Це була широкомасштабна атака з використанням усього набору російських кіберможливостей, щоб зруйнувати українську систему, але вона, на щастя, не мала успіху.

Досі найзначнішим кіберуспіхом Росії був вихід із ладу супутника KA-SAT компанії Viasat Inc. Це завдало значних збитків, які поширилися за межі України, але зрештою не дали Росії військової переваги. Атака могла бути задумана як частина більшої скоординованої кібератаки, яка виявилася безуспішною, або росіяни могли не очікувати на швидке відновлення обслуговування, яке було надано за допомогою ззовні.

Не дивлячись на все вище сказане тема кібергігієни в Україні є недостатньо дослідженою і навіть цих атак можна було б запобігти, якби кібербезпека краще вивчалась і контролювалась.

На відміну від України, в РФ поняття кібербезпеки та кібергігієни контролюється на держаному рівні. Стандартна російська тактика полягає у зламі баз даних або електронних листів, а потім їх витоку для отримання руйнівного ефекту. Іноді ці вкрадені дані фальсифікуються посилення ефекту. Ця тактика не спрацювала під час вторгнення РФ. Недостатньо російської пропаганди, щоб приховати незаперечні докази агресії, порушень міжнародного права та жахливих порушень прав людини, які були загальнодоступними з багатьох неурядових джерел. Пропаганда найбільш ефективна, коли вона використовує існуючі переконання, невдоволення чи скептицизм. Битва за контроль над розповіддю в основному відбувається в цифровому просторі і може визначатися діями у кіберпросторі. Увага Росії до того, щоб контролювати наратив про вторгнення, щоб відвести критику та заручитися суспільною підтримкою, відображає давню російську доктрину про важливість політичного та психологічного контексту конфлікту. Він інформує як про кібероперації, так і про операції радіоелектронної боротьби (РЕБ). Ці зусилля дали неоднозначні результати, і суперечка про оповідання залишається невирішеною. Він не мав успіху в Україні та серед прихильників України. Путін програв у західних демократіях і в Україні, але виграв у Росії і принаймні утримує свої позиції перед незахідною аудиторією в Китаї (за сприяння власної пропаганди та зусиль Китаю з контролю над наративом), Індії, Африці, на Близькому Сході та в деяких інших країнах (країни Латинської Америки).

Тема кібергігієни є дуже важливою та актуальною на сьогоднішній день. В Україні щоденно в засобах масової інформації з’являються новини про жертв інтернет-шахраїв чи втрату особистих даних чи акаунтів. Наприклад, в сусіда-загарбника серед молодшого покоління таке трапляється рідше, через привчання змалку до самостійної кібергігієни. Виконання такого роду тренінгів чи уроків покладається на місцеві або відповідальні за цю область державні органи влади. До речі, вже під час написання роботи, на ресурсі «Дія» в розділі «Освітні програми» з’явився розділ «Основи кібергігієни», що і підтверджує актуальність проблеми в наш час.

Знання з кібергігієни в мирний час необхідні, щоб протистояти хакерам, онлайн шахраям і не давати доступ до особистої інформації. Студентам та школярам, які навчаються у відповідних навчальних закладах, необхідно пояснювати що таке безпека особистих даних, чому вона важлива і що може статися, якщо стороння особа отримує доступ до них.

Отже, тема є надзвичайно важливю, бо знання з кібербезпеки в області кібергігієни можуть використовуватися як в мирний час, так і під час війни. Вони є досить сильною зброєю для того, щоб використовувати самим і зуміти захиститись від кібератак ворогів.

Метою дипломної роботи є дослідження процедури забезпечення кібергігієни в навчальних закладах, формування анкети розвитку, можливості покращення вже наявних способів забезпечення кібергігієни, а також надання власних рекомендацій щодо того, як змінити ситуацію з кібергігієною в Україні на краще.

РОЗДІЛ 1. АНАЛІЗ ПРОЦЕДУРИ ЗАБЕЗПЕЧЕННЯ ПРОВЕДЕННЯ КІБЕРГІГІЄНИ У НАВЧАЛЬНИХ ЗАКЛАДАХ

1.1 Кібербезпека школи

Із початком пандемії COVID-19, а потім повномасштабного вторгнення РФ в Україну, школи та університети перейшли на дистанційну форму навчання.

Всі учні користуються електронними девайсами, тому дуже важливо, щоб учні розуміли «кібергігієну». Кібергігієна — це набір принципів поведінки в Інтернеті, який запобігає порушенню вашої кібербезпеки.

Кібергігієна стосується фундаментальних найкращих практик кібербезпеки, які можуть застосувати фахівці та користувачі організації з безпеки. Відсутність кібергігієни може завдати шкоди безпеці учнів, а також безпеці шкільної системи в цілому.

Кожного року зростає кількість шкіл і коледжів, які серйозно постраждали від кіберінцидентів. Багато кіберінцидентів є нецільовими. Вони можуть вплинути на будь-яку школу, яка не має базового рівня захисту.

Школи зберігають багато конфіденційної інформації. Наприклад, банківські реквізити співробітників і батьків, медичні відомості про студентів, збереження документів, тощо. Все це має бути безпечним і конфіденційним.

Кіберзлочинці хочуть заробити гроші. Вони розуміють, що інформація організації часто є досить важливою для цієї організації і вони можуть бути готові заплатити викуп, щоб отримати її назад.

Хто стоїть за кібератаками?

1. Онлайн злочинці.

Вони справді добре вміють визначити, що і для чого можна монетизувати наприклад, крадіжка та продаж конфіденційних даних або зберігання систем та інформації з метою подальшого викупу.

2. Хакери

Нецільовим шляхом отримують доступ до особистих данних.

3. Зловмисні інсайдери

Використовують їхній доступ до даних або мереж організації здійснювати зловмисну діяльність, наприклад крадіжку особистої інформація для обміну з конкурентами.

4. Чесні помилки

Іноді персонал з найкращих намірів просто робить помилку, наприклад, надіславши електронною поштою якусь інформацію на неправильну електронну адресу.

5. Учні школи

Деяким учням просто подобається отримувати доступ до бази завдань аби отримати відповіді на контрольні і тести. [2]

Відсутність кібергігієни збільшує ризик кібератаки. За даними Stealth Labs, освіта була одним із найбільш вразливих секторів для кібератак, становлячи майже 64% усіх атак зловмисного програмного забезпечення, що доводить необхідність покращення кібергігієни в освіті. Тридцять відсотків користувачів у сфері освіти стали жертвами фішингу, свого роду кібератаки, коли кіберзлочинці видають себе за авторитетні компанії, щоб викрасти інформацію, таку як імена користувачів і паролі.[1]

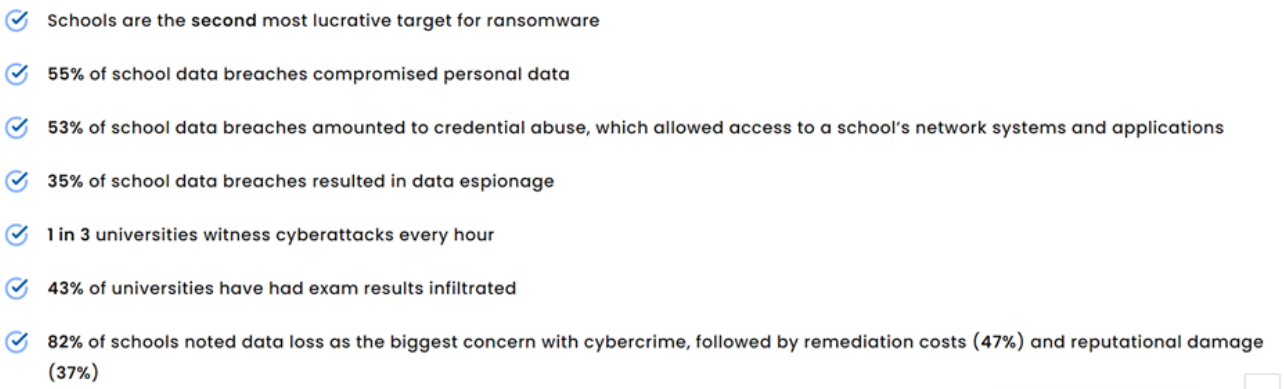

Рисунок 1.1 - Дані Stealth Labs щодо реалізації атак на освіту

Дистанційна освіта, яка стала необхідністю під час пандемії COVID-19, приносить із собою як переваги, так і певні ризики для кібергігієни школи. Ось кілька потенційних небезпек, з якими може стикатися шкільна кібергігієна в контексті дистанційної освіти:

1. Кібератаки та зловмисницькі дії: З дистанційною освітою з'являються нові можливості для кіберзлочинців, які можуть намагатися зламати систему, викрасти особисті дані учнів або завдати шкоди навчальному процесу. Це може бути виявлено у вигляді хакерських атак, фішингу, шкідливих програм та інших форм кіберзлочинності.

2. Недостатня кібербезпека платформ: Використання різноманітних платформ і інструментів для дистанційного навчання може створювати потенційні ризики, якщо ці платформи не мають достатнього рівня кібербезпеки. Недостатня захищеність даних учнів може призвести до незаконного доступу до особистої інформації чи її витоку.

3. Використання ненадійних джерел інформації: Учні можуть бути схильні до використання ненадійних джерел інформації під час самостійного навчання в дистанційному режимі. Це може призвести до поширення неперевіреної, неправдивої або ненадійної інформації, що впливає на якість навчання та розуміння певних тем.

4. Використання небезпечних програм та додатків: Учні можуть бути схильні до встановлення небезпечних програм або додатків на свої пристрої під час дистанційної освіти. Це може відкрити доступ до їхніх особистих даних або призвести до вразливості системи.

5. Відсутність контролю та нагляду: У дистанційному навчанні може бути важко забезпечити повний контроль і нагляд з боку вчителів та шкільних адміністраторів. Це може створювати можливість для небажаної поведінки, кібербулінгу, розповсюдження нецензурного матеріалу та інших небезпечних активностей.

Щодо різновидів кібератак, згідно ДСТУ ISO/IEC 27032:2012[3] виділимо основні ризики кібербезпеки, а саме:

— атаки соціальної інженерії;

— хакінг;

— розповсюдження шкідливого програмного забезпечення («шкідливого ПЗ»);

— шпигунське програмне забезпечення;

— інше потенційно небажане програмне забезпечення;

Дані ризики допоможуть нам зосередити увагу на безпеці кіберпростору та проблемах, які зосереджені на подоланні між різними сферами безпеки в кіберпросторі.

Для забезпечення кібербезпеки в контексті дистанційної освіти важливо використовувати надійні платформи, навчати учнів основам кібербезпеки, підтримувати відкритий канал комунікації між учнями, вчителями та батьками, а також забезпечувати адекватний контроль та нагляд.

Вчителі повинні навчати себе та своїх учнів про зловмисну кібердіяльність, щоб не стати жертвою таких схем. Вони повинні бути поінформовані і вивчати найкращі методи захисту себе та своїх учнів. Це є найкращим першим кроком до кібербезпеки. Розглянемо загрози учню на кожному з етапів його навчання в навчальному закладі.

1.1.1. Початкова школа (1-4 клас)

Відповідальність за забезпечення кібербезпеки в класах лягає на вчителів та батьків. В епоху, коли онлайн-інструменти, такі як Google Meets і Zoom стають невід'ємною частиною щоденного навчання дітей, потрібно завжди бути на вершині кібербезпеки.

Кібергігієна учнів початкових класів є важливим аспектом їхньої безпеки в онлайн-середовищі. Нижче наведено кілька ключових пунктів, що стосуються кібергігієни для молодших учнів:

1. Безпечне використання паролів: Учні повинні розуміти важливість міцних паролів і навчатися створювати унікальні паролі для своїх облікових записів. Вони

також повинні розуміти, що необхідно ніколи не розголошувати свої паролі іншим людям, навіть своїм друзям.

2. Безпека особистої інформації: Учні повинні бути свідомі про важливість захисту своєї особистої інформації, такої як ім'я, адреса, номер телефону тощо. Вони повинні знати, що ці дані необхідно залишати приватними і не розголошувати їх онлайн незнайомим людям.

3. Безпечне переглядання Інтернету: Учні повинні навчатися безпечно шукати інформацію в Інтернеті. Вони повинні розуміти, що необхідно перевіряти джерела інформації на достовірність та уникають небезпечних веб-сторінок.

4. Усвідомлення небезпек онлайн: Учні повинні розуміти, що інтернет може мати певні ризики, такі як шахрайство, кіберзнущання або небажані контакти. Вони повинні навчатися розпізнавати та уникати небезпек, розмовляти з дорослими про будь-які проблеми, з якими вони зіткнулися в Інтернеті.

5. Етика онлайн-поведінки: Учні повинні навчатися проявляти повагу та ввічливість в онлайн-середовищі. Вони повинні розуміти, що образи, залякування, цькування або розповсюдження приватних фотографій або відео є неприйнятними діями.

6. Повідомлення про проблеми: Учні повинні знати, як повідомляти про будь-які проблеми, з якими вони зіткнулися в онлайн-середовищі, своїм батькам, вчителям або іншим дорослим, яким вони довіряють.[11]

Загальний підхід до кібергігієни полягає у навчанні учнів про безпечне та відповідальне користування технологіями, вироблення у них навичок критичного мислення та розпізнавання потенційних загроз. Розуміння важливості кібербезпеки зміцнює їх здатність захистити себе в онлайн-середовищі, що дасть підвалини формування поведінки в кіберпросторі в майбутньому.

Найпростішими способами вирішення наявних проблем кібергігієни для учнів молодших класів можуть бути такими:

Навчання навичкам кібербезпеки в ігровій формі

Буде непросто домогтися того, щоб кожна дитина в класі активно та особисто вкладалася у підтримку гігієни кібербезпеки. Одним із найефективніших способів

подолання цього стала гейміфікація навчання навичкам кібербезпеки. Всі, від дошкільнят до 11-класників, що беруть участь у програмі, можуть завантажити та грати в ігри, які насправді вчать їх бути безпечнішими та захищеними в мережі.[16]

Інвестування у кращу фізичну безпеку

Забезпечуючи безпеку цифрового класу не потрібно забувати про те, що деякі школи почали впроваджувати гібридні онлайн-класи та очні заняття. Це означає, що учні можуть незабаром повернутися до школи. Школи можуть вкладають кошти в удосконалення, такі як голосові засоби зв'язку, камери та інші пристрої для керування доступом та входом у шкільну інфраструктуру і системи безпеки для працівників.

1.1.2 Середня школа (5-9 класи)

Хоча навчання в Інтернеті є найбезпечнішим методом навчання під час війни, воно також має кілька суттєвих недоліків. Діти страждають від фізичних і психічних наслідків онлайн-навчання, а також від дефіциту соціальних навичок. Якщо вчасно не вжити відповідних заходів, діти ризикують постраждати від пошкоджень на фізичному, психічному та соціальному рівнях.

Молоді люди і підлітки як правило, мають високий рівень технічних навичок самостійно, тому що вони стикалися з технологіями з раннього віку. Вони є впевненими користувачами соціальних мереж. Підлітки розуміються на техніці і проводять багато часу в Інтернеті.

Учні середньої школи знаходяться вже в більш свідомому віці і мають більше доступу до різних сайтів в інтернеті.

Кібергігієна учнів 5-9 класів є важливою складовою їхньої цифрової грамотності та безпеки в онлайн-середовищі. Основні аспекти, пов'язані з кібергігієною для учнів цього вікового діапазону, включають наступні:

Безпека соціальних мереж: Учні повинні навчатися безпечно використовувати соціальні мережі. Вони повинні розуміти, що необхідно бути обережними при прийнятті запитів на дружбу, обміну особистою інформацією та публікації

особистих фотографій або відео. Важливо наголосити на важливості повідомлення про будь-які неприємні або небезпечні ситуації.

Безпека електронної пошти: Учні повинні навчитися безпечно користуватися електронною поштою та розуміти, як уникати спаму, фішингових атак і вірусів. Вони повинні бути обережними при відкритті листів від незнайомих відправників і не повинні розголошувати особисту інформацію через електронну пошту.

Інформаційна безпека: Учні повинні розуміти важливість перевірки джерел інформації, особливо в Інтернеті. Вони повинні навчатися критично мислити і розпізнавати недостовірну або маніпулятивну інформацію. Розвиток навичок перевірки фактів та критичного осмислення інформації є важливим компонентом кібергігієни.

Кіберзнущання та кібербулінг: Учні повинні розуміти, що кіберзнущання та кібербулінг є неприйнятними діями. Вони повинні знати, як розпізнавати такі ситуації та як відповідати на них. Важливо виховувати емпатію, повагу та ввічливість в онлайн-середовищі.

Кібербезпека та конфіденційність: Учні повинні бути свідомими ризиків пов'язаних з конфіденційністю та особистою інформацією в онлайн-середовищі. Вони повинні навчатися захищати свої паролі, обмежувати доступ до особистої інформації та використовувати надійні налаштування приватності.[20]

Також вони можуть стати жертвами інших хакерів, які використовують такі платформи, як Facebook і WhatsApp, щоб заманити жертв на фішингові веб-сайти, які можуть скомпрометувати особисту інформацію. Також це можуть бути сайти соціальних мереж, але розроблені самими хакерами, так звані дзеркала. Це робиться для збору даних користувачів і їхнього майбутнього продажу. Різницею між реальним сайтом та дзеркалом може бути лише одна буква чи символ.

Кібергігієна учнів 5-9 класів вимагає постійного нагляду, навчання та взаємодії з батьками, вчителями та іншими дорослими, яким вони довіряють. Розуміння цих основних принципів допоможе учням стати більш безпечними та відповідальними користувачами цифрових технологій.

1.1.3 Старша школа (9-11 класи)

Великі проблеми з кібергігієною викликав раптовий перехід до дистанційного навчання, оскільки учні все частіше використовують свої персональні комп'ютери та незахищені мережі для участі в онлайн-класах, вектор загроз у секторі освіти збільшується.

Багато учнів старших класів мають настільну веб-камеру чи камеру, вбудовану в телефон, планшет чи ноутбук. На жаль, це може відкрити двері для «камфектінгу», коли хакери можуть отримати віддалений доступ і взяти під контроль веб-камеру.

Соціальна інженерія – шахрайство із соціальною інженерією є однією з головних загроз кібербезпеці, з якою стикаються учні старшої школи. Ці атаки ґрунтуються на маніпулюванні користувачами, щоб вони розкрили конфіденційну інформацію.

Після того як діти повертаються з позакласних занять, вони можуть брати з собою свій пристрій, щоб робити уроки на танцях або в спортзалі. Потрібно переконатися, що дитина підключається до Інтернету тільки через Wi-Fi, захищений паролем, адже після того, як (кіберзлочинець) проникне на пристрій дитини, що знаходиться у домашній мережі, він зможе проникнути на інші пристрої у цій мережі, які цілком можуть бути робочим комп'ютером. Студентам необхідно часто міняти свої паролі, перевіряти особистість людей в Інтернеті та уникати підключення до незахищених мереж WIFI.

Кібергігієна учнів 9-11 класів є ключовою у сучасному цифровому світі і включає в себе ряд аспектів, які їм потрібно розуміти та практикувати:

Кібербезпека: Учні повинні мати свідомість про різні види кіберзагроз, такі як хакерські атаки, шкідливе програмне забезпечення, шпигунське програмне забезпечення. Вони повинні навчитися захищати свої особисті дані, паролі та конфіденційну інформацію, а також використовувати антивірусні програми та оновлювати своє програмне забезпечення.

Соціальні мережі та приватність: Учні повинні бути усвідомлені про наслідки розголошення особистої інформації та зображень в соціальних мережах. Вони повинні навчитися встановлювати належні налаштування приватності, обмежувати доступ до своїх профілів та розуміти, які типи інформації можуть стати предметом цифрової незгоди або кіберзнущання.

Критичне мислення і перевірка інформації: Учні повинні навчитися перевіряти достовірність інформації, зокрема в Інтернеті. Вони повинні розуміти, як розпізнавати фейкові новини, маніпулятивну інформацію та стереотипи. Розвиток критичного мислення допомагає їм зрозуміти складнощі та потенційні небезпеки цифрового світу.

Етика інтернет-комунікацій: Учні повинні розуміти етичні аспекти спілкування в онлайн-середовищі. Вони повинні знати, як підтримувати повагу до інших, уникати кіберзнущання та кібербулінгу, а також бути обережними з образами та ненависницькою мовою.

Цифровий слід: Учні повинні розуміти, що кожна їх дія в Інтернеті залишає слід. Вони повинні бути усвідомлені своєї цифрової сліду та наслідків, які вона може мати для їх майбутньої кар'єри та особистого життя. Важливо вчити учнів контролювати свої дії та відповідально використовувати цифрові технології.[10]

Кібергігіна учнів 9-11 класів спрямована на розвиток їх цифрової грамотності, самосвідомості та вмінь використовувати цифрові технології відповідально та етично. Розуміння цих аспектів допомагає їм стати освіченими та безпечними учасниками цифрового світу.

1.2 Фішингові повідомлення з соціальних мереж та сайтів продажу

Вважаю за потрібне, окремо виділити у роботі проблему фішингових повідомлень в соціальних мережах та на сайтах продажів. Вони є дуже небезпечними, адже зазвичай зроблені якісно і зовні їх майже не відрізнити від служби підтримки чи оформлення доставок на оригінальному сайті. Наприклад, такі псевдосайти небезпечні такими загрозами як викрадення особистих даних чи втрата

банківських рахунків або даних. Тому вважаю за доцільне окремо зупинитися на даній темі більш поглиблено.

Хоча в цілому ми не можемо відносити даний підрозділ до кібербезпеки школи як структури, але даний тип атак є небезпечним для суб'єктів, які знаходяться, працюють, навчаються в навчальних закладах. [6]

Фішингові повідомлення на Facebook та WhatsApp

Facebook та WhatsApp наразі перебувають на провідних місцях в звіті про найбільш експлуатовані адреси сайтів (Рисунок. 1.2).

#	Brand	Unique Phishing URLs	QoQ Growth
1	- PayPal Category: Financial Services	11,392	-31.2%
2	↑2 Facebook Category: Social Media	9,795	-18.7%
3	↓1 Microsoft Category: Cloud	8,565	-38.2%
4	↓1 Netflix Category: Cloud	6,758	-50.2%
5	↑63 WhatsApp Category: Social Media	5,020	13,467.6%
6	↓1 Bank of America Category: Financial Services	4,375	-21.5%
7	↑1 CIBC Category: Financial Services	2,414	11.2%
8	↑4 Desjardins Category: Financial Services	2,243	54.4%
9	↓3 Apple Category: E-Commerce/Logistics	2,126	-57.9%
10	↓1 Amazon Category: E-Commerce/Logistics	2,110	0.6%

Рисунок 1.2 - Найбільш експлуатовані фішерами адреси сайтів

Тож зважаючи на те, що розглядається тема кібергігієни та рекомендації для учнів шкіл, ми можемо включити приклади фішингу в Facebook та WhatsApp, які можуть безпосередньо стати загрозою для учнів навчальних закладів. Ось декілька прикладів:

1. Фальшиві вимоги відновлення пароля: Користувач може отримати електронного листа або повідомлення від Facebook або WhatsApp, яке запрошує його змінити або відновити пароль. Шахраї можуть використовувати підроблені веб-сторінки або форми для збору особистих даних, таких як ім'я користувача та пароль, з метою зламу акаунта або використання цих даних у шахрайських цілях.

2. Фішингові посилання через повідомлення: Шахраї можуть надсилати повідомлення з підробленими посиланнями, які просують користувача натиснути на них. Ці посилання можуть направляти на шахрайські веб-сторінки, де шахраї можуть намагатися збирати особисту інформацію або виконати шкідливі дії на пристрої користувача(Рисунок 1.3).

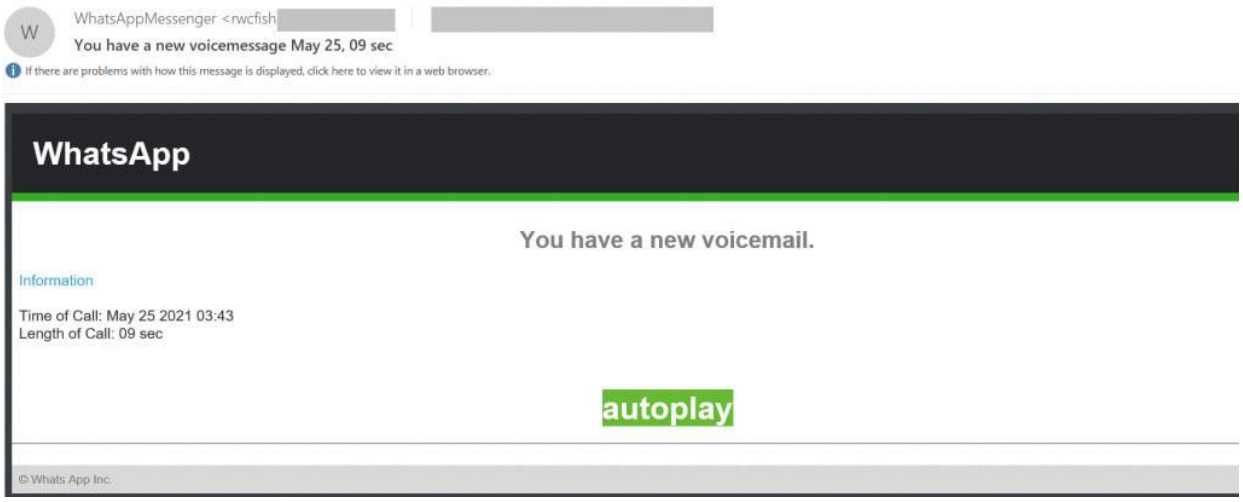

Рисунок 1.3 - Повідомлення від невідомого контакту з нібито голосовим повідомленням з подальшим перенаправленням в браузер

3. Фальшиві оповіщення про небезпеку аканту або про пропозицію від компанії: Користувач може отримати повідомлення, в якому його запевняють, що його акаунт або дані на Facebook або WhatsApp знаходяться під загрозою. Шахраї можуть намагатися отримати від користувача його особисту інформацію або навести на думку, що йому потрібно змінити свої дані для попередження будь-яких проблем. Або під виглядом заманливих пропозицій збирати дані користувачів, обіцяючи за це певні бонуси чи винагороди (Рисунки 1.4 - 1.6).

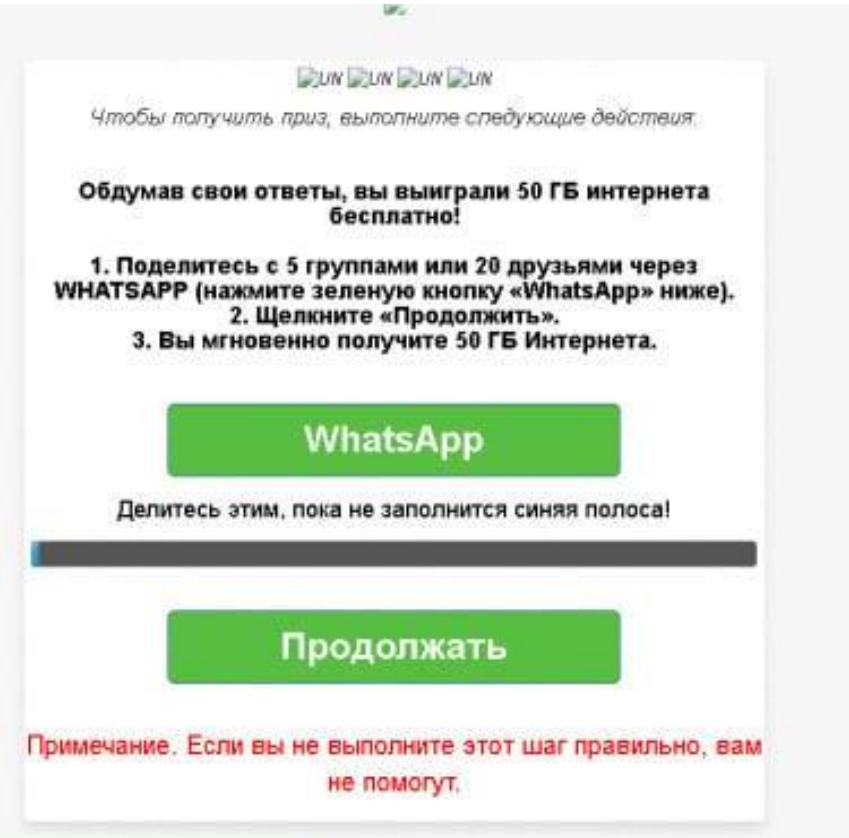

Рисунок 1.4 - Приклад розсилки під виглядом лотереї

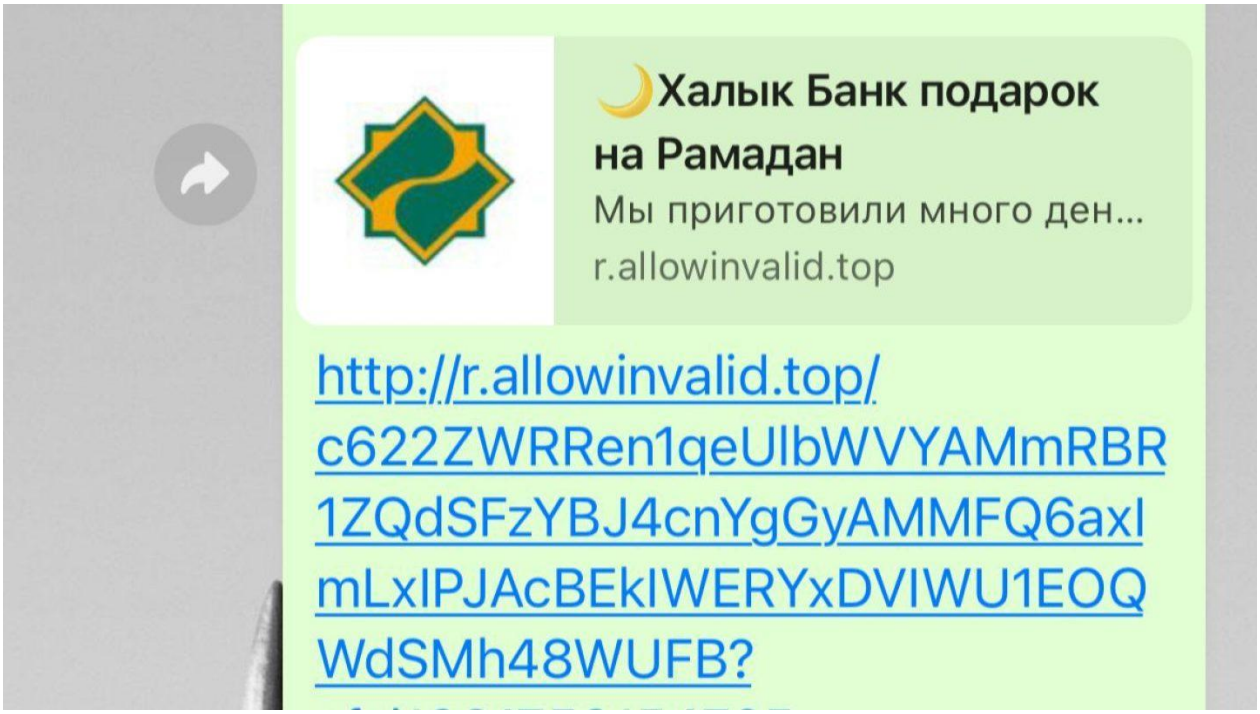

Рисунок 1.5 - Приклад фішингового повідомлення з невідомого ресурсу під виглядом пропозиції від банку

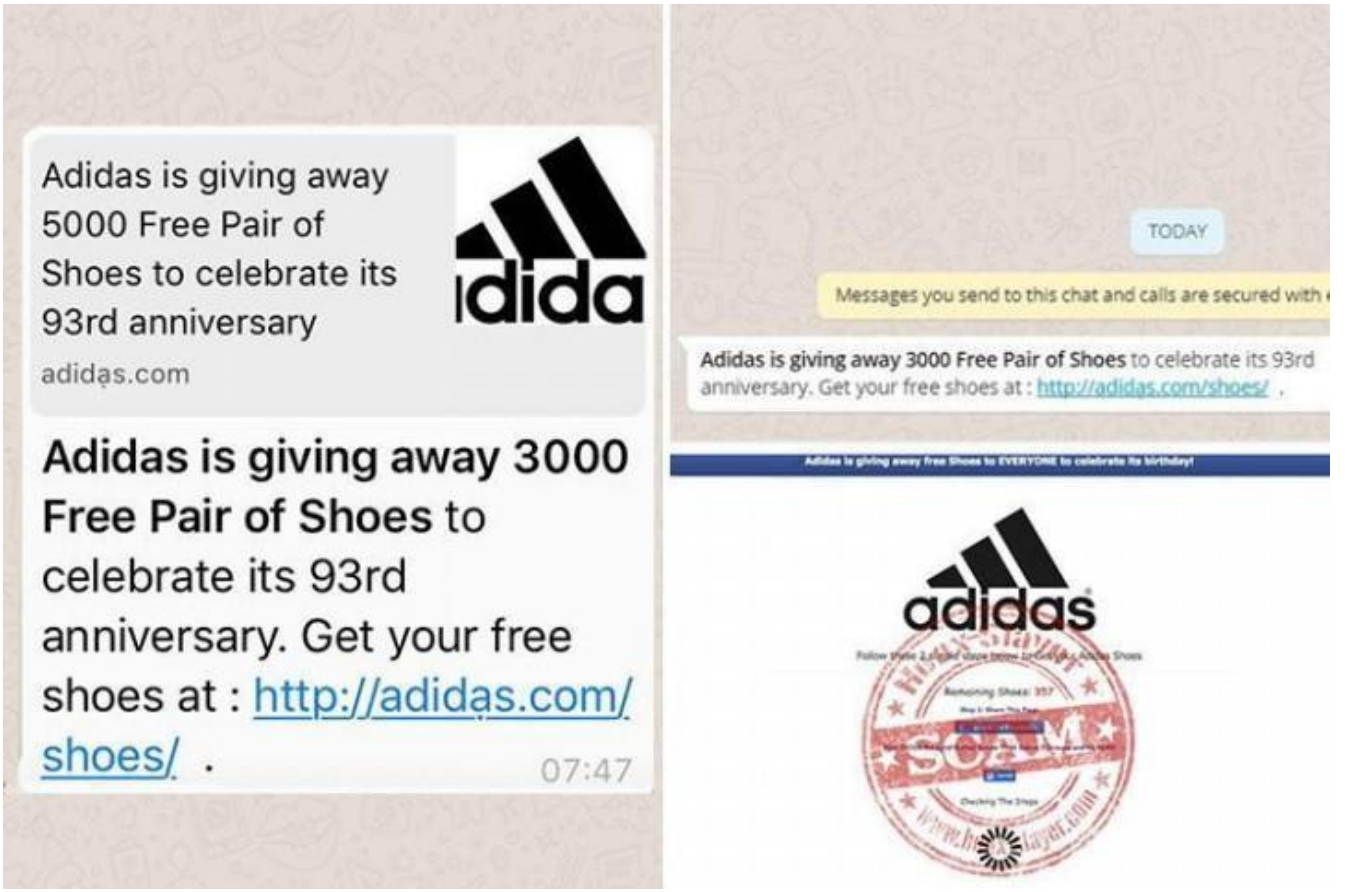

Рисунок 1.6 - Під виглядом акції проводиться збір даних користувачів, через їхні ж поширення

4. Підроблені повідомлення від знайомих: Шахраї можуть підробити профілі користувачів Facebook або WhatsApp та надсилати повідомлення від їхніх імен. Ці повідомлення можуть містити посилання на шахрайські веб-сторінки або запити про надання особистої інформації, фінансових даних або навіть прохання про переказ коштів. Іноді вас просто можуть додати невідомі в групу з матеріалами порнографічного характеру (Рисунок 1.7).

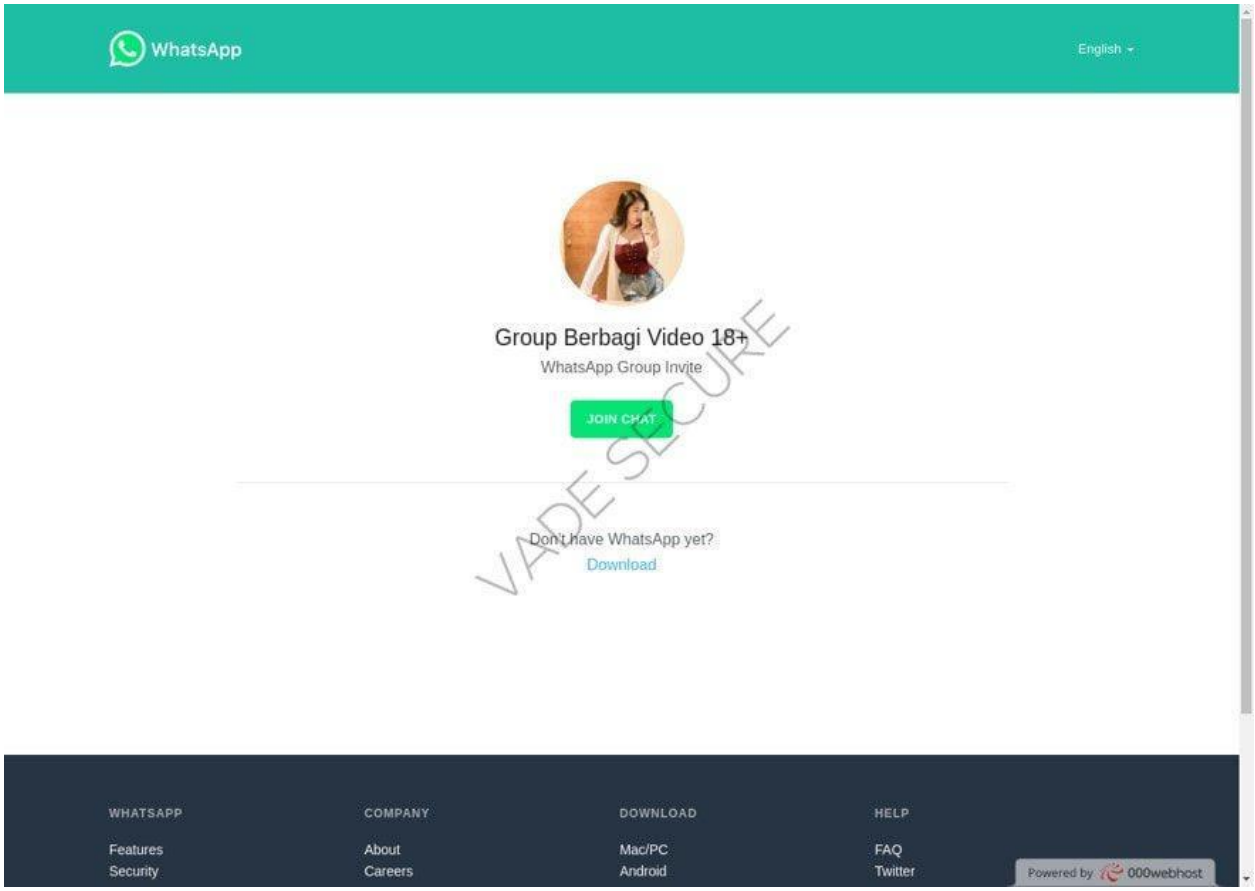

Рисунок 1.7 - Додавання в невідому групу з неприйнятним контентом

Важливо пам'ятати, що це лише кілька прикладів фішингу в Facebook та WhatsApp, і шахраї постійно вдосконалюють свої методи.

Фішингові повідомлення на olx.ua,

Фішингові повідомлення є поширеним видом шахрайства, яке може відбуватися із сайту продажів. Розглянемо на прикладі найпопулярного серед шахраїв в Україні, таких як olx.ua. Ось декілька прикладів фішингу, з якими можуть зіштовхнутися користувачі цих платформ:

1. Фальшиві пропозиції продажу: Шахраї можуть розміщувати оголошення на olx.ua з привабливими цінами на товари, які насправді не існують або є підробленими. Вони можуть надсилати користувачам повідомлення з проханням здійснити попередню оплату або вказати свої особисті дані, заявляючи, що це потрібно для оформлення покупки (Рисунки 1.8 – 1.10).

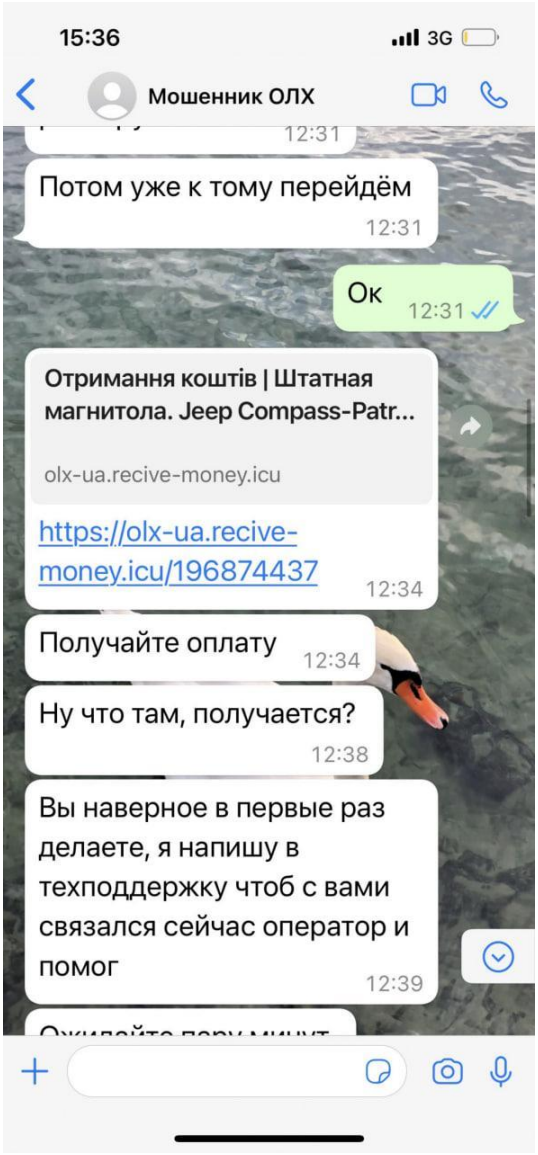

Рисунок 1.8 - Приклад листування з шахраєм

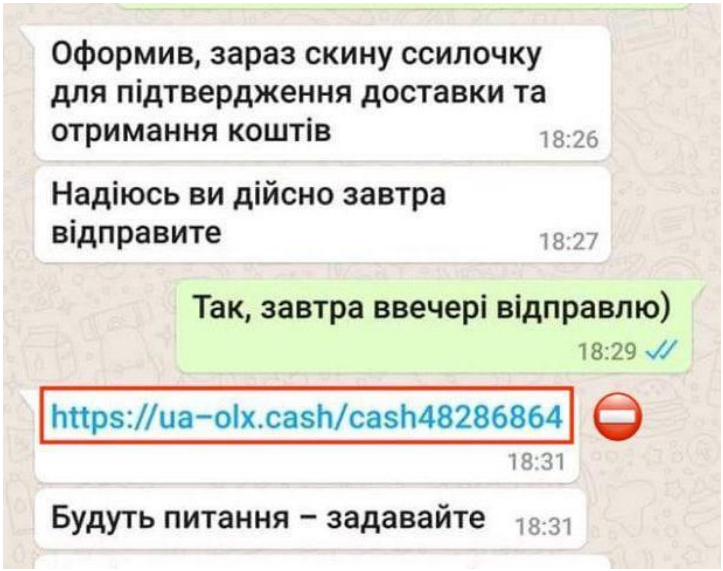

Рисунок 1.9 - Приклад підозрілого сайту з метою збору банківських даних

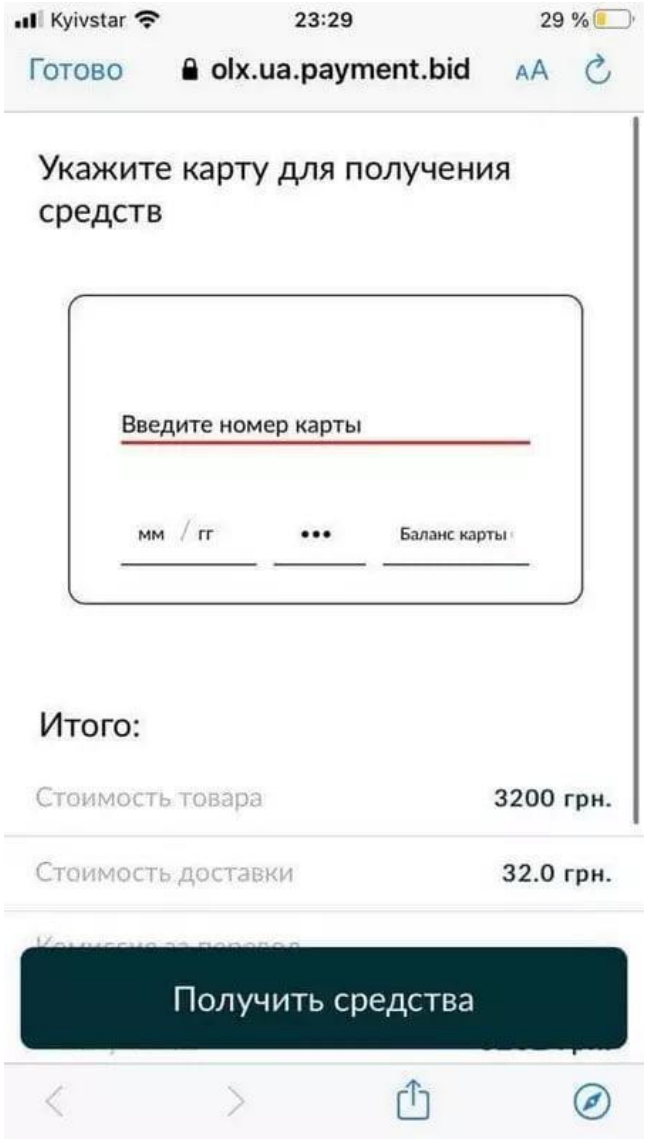

Рисунок 1.10 - Інтерфейс підозрілого сайту з метою збору банківських даних

2. Вимоги попередньої оплати: Шахраї можуть звертатися до користувачів olx.ua з пропозиціями про купівлю товару за заниженою ціною або з доставкою відомих служб. Вони можуть вимагати попередню оплату за товар або послугу, але після отримання платежу зникнути без надання товару або надати підроблені товари.

3. Фальшиві повідомлення від платіжних систем: Шахраї можуть відправляти електронні листи або повідомлення, які виглядають, ніби вони від репутованих платіжних систем, наприклад, PayPal чи Privat24. Вони можуть надсилати посилання, які ведуть на підроблені веб-сторінки, де шахраї намагаються зловживати фінансовою інформацією користувача.

4. Фальшиві лотереї та акції: Шахраї можуть надсилати повідомлення, в яких повідомляють, що користувач нібито виграв лотерею або акцію на olx.ua, і щоб отримати бажаний приз, необхідно надати власні банківські дані для "перерахунку коштів".

5. Псевдо-клієнти та шахрайські угоди: На olx.ua, шахраї можуть пропонувати угоди з продажу товару, але вимагати зустрічі в небезпечних місцях або вимагати передплату на послуги з доставки або оплати резерву товару. У деяких випадках, після отримання грошей, шахраї можуть відмовлятися від угоди або надавати підроблені товари.

Важливо пам'ятати, що це лише кілька прикладів фішингу, які можуть виникати на olx.ua та Rozetka. Шахраї постійно адаптують свої підступи, тому важливо бути дуже обережними. Злочинці використовують дані платформи, через низьку кібербезпечність їх користувачів та можливість ускладнити шлях пошуку їхнього сліду в інтернеті.

Висновок до розділу 1

В результаті аналізу літератури, законодавчої бази, стану кібергігієни в Україні та навчальних закладах, визначено групи злочинців, які полюють на певного роду дані користувачів ,було поділено учнів на певні групи, залежно від загроз на кожному етапі їх навчання, розглянуто поглиблено аспекти їхньою кібергігієни такі як: безпечне використання паролів, безпека особистої інформації, безпечне переглядання Інтернету, усвідомлення небезпек онлайн, етика онлайн-поведінки, безпека соціальних мереж, безпека електронної пошти, інформаційна безпека, кіберзнущання та кібербулінг, кібербезпека та конфіденційність, «камфектінг», соціальна інженерія, незахищені мережі інтернету, цифровий слід, недбале ставлення до дозволів програм та політик безпеки програм. Особливу увагу приділено такому різновиду кібератак, як фішинг, через його зростаючу популярність серед зловмисників, зокрема наглядно продемонстровано рисунками

приклади реалізації фішингових атак через соціальні мережі Facebook та WhatsApp та сайту продажів olx.ua.

РОЗДІЛ 2. ПРОВЕДЕННЯ ЕКСПЕРИМЕНТУ ЩОДО КІБЕРБЕЗПЕЧНОЇ ПОВЕДІНКИ СЕРЕД УЧНІВ ПОЧАТКОВОЇ, СЕРЕДНЬОЇ І СТАРШОЇ ШКОЛИ

Шкільні системи можуть взяти до уваги той факт, що окремі особи та компанії, які використовують розумні пристрої, все частіше стають жертвами кіберзлочинців. Стан кібергігієни в українських школах наразі є предметом значної уваги, оскільки зростаюча залежність від технологій та поширення Інтернету ставлять перед учнями нові виклики та загрози. Однак, необхідно врахувати, що інформація про стан кібергігієни в українських школах може бути обмеженою, оскільки офіційна статистика та дослідження в цій галузі не завжди доступні або знаходяться на етапі розвитку.

Про стан кібергігієни свідчать загальні тенденції та виклики, що стосуються кібергігієни в українських школах: обмежені ресурси та недостатня увага до кібербезпеки, свідомість та навички учнів, тощо.

Літератури про те, як успішні учасники в розвинутих країнах, таких як Україна, вивчають навички кібербезпеки під час навчання, дещо небагато. Не дивлячись на наявність навчально-методичних матеріалів, розширення сфери навчання в галузі інформатики пройшло. Таким чином, це дослідження показує, наскільки українські учні розвивають кібербезпечну поведінку в початковій, середній та старшій школі та як вони набувають досвіду – самостійно, з допомогою вчителів чи їхнього оточення. Ця анкета використовується для самооцінки інформації у сфері кібербезпеки та перевірки власних набутих навичок. Результати дослідження показують, що українські шкільні програми приділяють мало уваги цій темі, і учні в основному отримують онлайн-навчання через досвід, Інтернет-навчання, батьків, братів і сестер. Крім того, з часом багато студентів почали поводитися більш необачно. Окремий наголос потрібно зробити на темі виявлення фішингових листів і фішингових сайтів. Учнів потрібно переконати, що ризикована поведінка в Інтернеті може бути контрпродуктивною для них самих та організацій, до яких вони належать.[18]

2.1 Метод та анкета розвитку

Анкетування учнів стосовно кібергігієни має кілька сильних сторін, серед яких можна виділити наступні:

1. Збір об'єктивних даних: Анкета дозволяє зібрати кількісні дані щодо рівня кібергігієни учнів. Це дозволяє отримати об'єктивне уявлення про їхню поведінку в кіберпросторі, виявити основні проблеми та потреби, а також оцінити ефективність заходів щодо кібербезпеки.

2. Анонімність і конфіденційність: Анкета забезпечує анонімність відповідей учнів, що дозволяє їм вільно висловити свої думки та досвід без страху перед можливими наслідками чи судженнями. Крім того, гарантується конфіденційність зібраних даних, що сприяє довірі та відкритості учнів під час заповнення анкети.

3. Широкий охоплюючий спектр: Анкета може охоплювати різні аспекти кібергігієни, включаючи знання про кібербезпеку, навички поведінки в Інтернеті, усвідомлення ризиків та захист від них. Це дозволяє отримати комплексне уявлення про стан кібергігієни серед учнів.

4. Виявлення потреб і проблем: Анкета допомагає виявити потреби та проблеми, з якими зіштовхуються учні в кіберпросторі. Це може стати основою для розробки та впровадження спеціалізованих програм та заходів щодо підвищення кібергігієни учнів.

5. Моніторинг прогресу: Проведення анкетування учнів щодо кібергігієни може бути повторюваним процесом, що дозволяє виявляти зміни в їхній поведінці та усвідомленні ризиків з часом. Це дозволяє моніторити прогрес учнів і оцінювати ефективність впроваджених заходів з кібербезпеки.

6. Включення учнів до процесу: Заповнення анкети дозволяє учням активно брати участь у формуванні безпечного кіберпростору. Вони мають можливість поділитися своїми думками, досвідом та пропозиціями, що сприяє почуттю власної важливості та залученості до процесу.

7. Персоналізація: Анкета може бути адаптована до різних груп учнів залежно від їхнього віку, рівня знань та досвіду в кіберпросторі. Це дозволяє отримати більш точну інформацію про потреби та особливості кожної групи учнів.

8. Виявлення трендів: Анкетування учнів щодо кібергігієни може допомогти виявити тренди та зміни в поведінці учнів в кіберпросторі. Це дозволяє налагодити відповідні програми та заходи, щоб відповідати сучасним викликам і загрозам в цій сфері.

9. Взаємодія зі стейкхолдерами: Анкетування учнів щодо кібергігієни може включати не лише учнів, але й батьків, вчителів та адміністраторів навчальних закладів. Це створює можливість для взаємодії і спільного вирішення проблем кібербезпеки на різних рівнях.

10. Підвищення свідомості: Заповнення анкети стимулює учнів докладати увагу до своєї кібербезпеки та ставлення до навколишнього кіберсередовища. Це допомагає підвищити їхню свідомість про потенційні ризики та впливає на зміну їхньої поведінки в Інтернеті.

11. Планування і розробка стратегій: Результати анкетування можуть послужити основою для розробки стратегій та планування заходів щодо покращення кібергігієни учнів. Це дозволяє належним чином спрямувати ресурси і зусилля для покращення кібербезпеки в навчальних закладах.[19]

Основними кроками анкетного методу аналізу стану кібергігієни в навчальному закладі є:

1. Розробка анкети: Спочатку потрібно розробити анкету, в якій визначаються цілі дослідження і формулюються запитання, що стосуються кібергігієни. Запитання можуть охоплювати такі аспекти, як знання про кібербезпеку, усвідомлення ризиків, використання паролів, безпека особистих даних, рівень набутих навичок, джерела знань, тощо.

2. Проведення анкетування: Після розробки анкети, вона може бути розіслана учням для заповнення. Анкету можна провести в письмовій формі, електронною поштою, через онлайн-платформи або спеціальні анкетні інструменти.

3. Аналіз результатів: Після отримання заповнених анкет, необхідно проаналізувати отримані дані. Це включає підрахунок відповідей, визначення частоти відповідей на окремі запитання, виявлення загальних тенденцій та закономірностей.

4. Інтерпретація результатів: Після аналізу даних слід здійснити інтерпретацію результатів. Це означає виявлення сильних та слабких сторін у стані кібергігієни в навчальному закладі, виявлення проблемних областей та потреб у покращенні кібербезпеки.

5. Розробка рекомендацій: На основі отриманих результатів можна розробити рекомендації та стратегії для покращення кібергігієни в навчальному закладі. Це може включати проведення навчальних програм, тренінгів, впровадження політик безпеки, інформаційні кампанії тощо.

Сильні сторони анкетного методу аналізу стану кібергігієни в навчальному закладі включають його простоту в застосуванні, можливість швидкого збору даних великої кількості учнів і отримання об'єктивної оцінки стану кібербезпеки. Крім того, анкети можуть бути анонімними, що дозволяє учням бути більш відкритими у своїх відповідях.

Однак, анкетний метод також має свої обмеження. Наприклад, відповіді учнів можуть бути підконтрольовані та не завжди відображати їхню реальну поведінку. Також, існує ризик неправильного розуміння запитань або недостатньо точних відповідей. Крім того, анкети не забезпечують можливості для детального вивчення контексту та глибини проблеми, що можуть вимагати додаткових дослідницьких методів, таких як спостереження або інтерв'ю. Детальніше про дані аспекти можна буде сказати лише після створення і успішного анкетування учнів навчальних закладів.

Тобто, анкетний метод є цінним інструментом для аналізу стану кібергігієни в навчальному закладі, проте його використання слід поєднувати з іншими методами та ураховувати його обмеження, які, як було сказано раніше, можуть залежати від різних чинників.

Анкетування учнів щодо кібергігієни є цінним інструментом, який допомагає отримати інформацію про поведінку та усвідомлення учнів стосовно кібербезпеки. Це допомагає розуміти потреби учнів навчальних закладів і розробляти ефективні програми та заходи для забезпечення їхньої безпеки в кіберпросторі, а відповідно і знизити ризики для систем безпеки навчальних закладів і їх працівників.

Перейдемо до самого методу дослідження теми. Проведено анкетне кількісне оцінювання поведінки учнів початкової та середньої школи та виявлено відмінності між цими двома групами. Для спрощення краще, об’єднати середню та старшу шкільні групи, адже як показують результати, відмінності між поведінкою в кіберпросторі є мінімальними, зате проблеми в обох груп учнів спільні. Для покращення інтерпретації результатів були проведені групові інтерв’ю [21].

Ця анкета була розроблена на основі оціночних анкет, використаних у попередніх дійсних дослідженнях. Не було знайдено досліджень щодо навчання дітей безпеки в Інтернеті в Україні. Таблиця 1 підсумовує вивчені питання безпеки (ISA). Виділені шість характеристик. Ці характеристики включають, скільки пунктів містить опитувальник, чи має опитувальник теоретичну основу, який опитувальник був випущений для використання, рік публікації опитувальника, що вимірює опитувальник і якою є цільова аудиторія опитувальника.

Таблиця 1

Вивчені питання безпеки опитаними

Характеристики	UISAQ	BCISQ	OSBBQ	Чотири шкали	HAIS-Q
Заходи	Рівень поінформованості про безпеку	Інформаційна безпека та обізнаність	Поінформованість про кібербезпеку, ставлення, поведінку та переконання.	Поведінка та обізнаність у сфері особистої інформаційної безпеки	Поінформованість про інформаційну безпеку
Теоретична основа	Ніхто	Ніхто	Модель переконань про здоров'я	Ніхто	КАБ модель

			та теорія захисної мотивації		
Цільова група	Школярі	Кожен	Співробітники	Співробіт-ники та школярі	Співробіт-ники та школярі
Доступність	Ні	Ні	Ні	Так	Так
Предмети	33	17	75	89	63

2.1.1 Процедурна анкета

Опитування проводилися в групах випускних класів початкової школи (учні 6-10 років) та середньої та старшої школи (учні 11-17 років). На момент закінчення середньої школи учні мають вік від 16 до 17 років. Кар'єрна технічна або вища освіта доступна після закінчення середньої школи. Програма Google Forms використовується для опитувань, щоб уникнути помилок реплікації. Учні отримали посилання від свого вчителя, щоб пройти опитування на уроці. Тому дослідники не бачили імен студентів. Дані, які можуть ідентифікувати студента, зберігаються. Щоб забезпечити безперебійний збір даних, дослідник (тобто перший автор) був присутній особисто або віртуально під час опитування. Після прибуття дослідника ознайомили з темами та основними напрямками дослідження. Він сказав студентам, що опитування було анонімним. Студентам заборонено спілкуватися під час розслідування. Якщо вони не розуміють предмет, вони можуть звернутися до дослідника за поясненнями.

Дана анкета може бути адаптованою не лише під учнів навчальних закладів, а і студентів вищих навчальних закладів, працівників державних установ, а також для працівників комерційних компаній.

2.1.2 Анкетний метод аналізу

Анкетний метод аналізу стану кібергігієни в навчальному закладі є ефективним інструментом для збору інформації про ставлення учнів до

кібербезпеки та їхню поведінку в кіберпросторі. Цей метод використовує стандартизовані запитання, які адресують різні аспекти кібергігієни, щоб отримати об'єктивну оцінку поточного стану.

Анкета аналізувалася по пунктам. Нулева гіпотеза включалася в тому, що немає ніяких відмінностей між поведінкою учнів початкової школи і старшокласників у відношенні кібербезпеки. Щоб вирахувати рівень значущості для кожного окремого тесту в цій ситуації з кількома тестами, спочатку вибраний рівень 5% був розділений на кількість елементів, відомих як поправка Бонферроні, і в результаті $\alpha = 0,05/16 = 0,003125$. Якщо p - значення елемента було менше, ніж $\alpha = 0,003125$, то різниця була значущою. Величину ефекту інтерпретували на предмет значущих відмінностей з використанням коефіцієнта Коена (Norman & Streiner, 2003). Далі Коену величина ефекту d інтерпретувалася наступним чином: від 0,2 до 0,5 — малий, від 0,5 до 0,8 — середній і вище 0,8 — великий.

2.1.3. Результати

Начальна школа

В результаті досліджень було виявлено що учні початкової школи обережно ставляться до своєї поведінки в Інтернеті. Наприклад, не повідомляють власні паролі однокласникам, не натискають посилання в електронних листах і не відкривають вкладені файли, не враховуючи потенційні ризики. Крім того, у школі ми не шукаємо все, що хочемо, в Інтернеті. Більшість учнів початкової школи, які беруть участь, консультуються з батьками, коли стикаються з дивними подіями в Інтернеті.

Однак завантаживши усе, що потрібно для шкільних завдань, можуть забути вимкнути електронні пристрої належним чином, або просто не заблокувати їх. Що стосується поведінки паролів, учні початкової школи, як правило, використовують надійні паролі та використовують різні паролі для соціальних мереж і шкільних облікових записів, але трапляються стандартні випадки «одного пароля на все», що знижує рівень їхньої безпеки.

Фішингові електронні листи та фішингові веб-сайти для учнів даної групи тяжко виявити. Вони також не оцінюють належним чином безпеку веб-сайтів перед тим, як вводити їх дані. Учні доводять, що не публікують усе, що хочуть опублікувати про свою школу, але вони не отримують достатньо інформації про наслідки власних дій в соціальних мережах.

Середня та старша школа

Здебільшого основними факторами, які повпливали на результати опитування можна назвати власну освіченість, досвід та рівень інтернет-культури кожного з них. Старшокласники добре відповіли на запитання про поведінку паролів. Вони мають надійні паролі, використовують різні паролі для соціальних мереж і шкільних облікових записів і не повідомляють паролі однокласникам.[9]

Старшокласники також добре відповіли на запитання про поведінку електронною поштою. Вони не натискають на посилання в електронних листах, вони не відкривають вкладені файли або перевіряють ресурси, з яких надійшло підозріле повідомлення.

Також можуть виявляти фішингові електронні листи та фішингові веб-сайти. Однак вони не оцінюють належним чином безпеку веб-сайтів перед тим, як вводити інформацію чи завантажувати все, що їм потрібно для шкільних завдань. Вони публікують усе, що хочуть про школу, і не розглядають наслідки, які можуть повпливати на їхнє життя і життя навчального закладу як цілісної структури, перш ніж публікувати щось у соціальних мережах.

Варто відмітити, що старшокласники, тримають свої електронні пристрої заблокованими під час уроку в більшості випадків. З іншого боку, старшокласники шукають чим зайнятися в школі, тому вони нерегулярно перевіряють налаштування конфіденційності своїх акаунтів у соціальних мережах, що свідчить про їхню надмірну самовпевненість у власній кібербезпеці та нехтування правилами кібергігієни.

Висновок до розділу 2

В результаті пройдених раніше етапів було сформовано анкету розвитку, на основі проведених раніше опитувань. Було розглянуто результати опитування і визначено позитивні моменти і недоліки кібербезпеки груп учнів навчальних закладів. Задля зручності, після аналізу проведених раніше опитувань групи учнів середньої та старшої школи було вирішено об'єднати через схожість проблем і позитивних результатів згаданих раніше груп учнів навчальних закладів.

РОЗДІЛ 3. ОБГОВОРЕННЯ ЕКСПЕРИМЕНТАЛЬНИХ ДАНИХ

При порівнянні старшої та молодшої шкіл, важливо зазначити, що старшокласники краще виявляли фішингові сайти та електронні листи. Значна різниця була виявлена для обох елементів, і розмір ефекту для цієї різниці був помірним. Що старшокласники вміють найкраще, так це блокувати свої електронні пристрої.

З іншого боку, старшокласники впоралися з певними проблемами гірше, ніж учні початкової школи. Старшокласники частіше шукали те, що їм подобається, у пункті «пошук в Інтернеті в школі». Крім того, з пунктом «завантажити все, що потрібно для шкільних завдань», старшокласники впоралися гірше.

3.1 Результати кількісної частини дослідження

Ці результати стосуються основних відмінностей між учнями початкової та старшої школи та завдань, з яких обидві групи показали погані результати. Ці результати були використані як вхідні дані для фокус-групових інтерв'ю. Таблиця з результатами наведена у додатку.

3.2 Результати якісної частини досліджень

При аналізі змісту групових інтерв'ю виникли дві теми. Такими темами були «Джерела безпечної поведінки» та «Небезпечна поведінка».

3.2.1 Ресурси для навчання безпечній поведінці.

Загалом, навчання з особистого досвіду використовувалося найчастіше для розвитку кібербезпечної поведінки. Наприклад, більшість респондентів назвали власний досвід як джерело для того, щоб навчитися розпізнавати фішинг, тоді як

деякі посилалися на вплив своїх батьків, а один також згадав школу. Крім того, п’ятеро учнів пригадали випадки, пов’язані з блокуванням своїх пристроїв, вказуючи на те, що вони заблокували свої пристрої через події у школі.

Визначено кілька джерел, які сприяють безпечній поведінці учнів навчальних закладів в кіберпросторі. Ось деякі з них:

Навчальні заклади: Школи та інші навчальні заклади можуть впроваджувати програми з кібербезпеки та кібергігієни в своїх навчальних планах. Це може включати в себе вивчення основних принципів безпеки в Інтернеті, правил поведінки в соціальних мережах, захисту від кіберзлочинів та інші важливі аспекти.

Родина: Батьки та опікуни мають велике значення у формуванні безпечних поведінкових звичок у своїх дітей в кіберпросторі. Вони можуть бути відповідальні за надання належної інформації про кібербезпеку, контролювання використання Інтернету та навчання учнів правилам безпеки в онлайн-середовищі.[4]

Організації та громадські ініціативи: Різні організації та громадські ініціативи займаються популяризацією кібербезпеки та кібергігієни серед учнів. Вони проводять тренінги, семінари, лекції та інші заходи, спрямовані на надання необхідних знань та навичок для безпечного користування Інтернетом.

Онлайн-ресурси: Існують численні онлайн-ресурси, які надають матеріали, посібники, відео та інші інформаційні ресурси з кібербезпеки та кібергігієни для учнів. Ці ресурси можуть бути доступними як учням, так і вчителям, і допомагають підвищити рівень усвідомлення про безпеку в Інтернеті.

Соціальні мережі та спільноти: Соціальні мережі та онлайн-спільноти можуть також виступати джерелом інформації та підтримки учням у питаннях кібербезпеки. Вони надають можливість обмінюватися досвідом, отримувати поради та рекомендації від інших учасників, які цікавляться цією темою.[7]

Ці джерела допомагають учням отримати необхідні знання, розуміння та навички для безпечного та відповідального користування Інтернетом.

3.2.2 Небезпечна поведінка

Під час співбесід було виявивлено, що більшість студентів були самовпевненними. Майже всі учасники сказали, що вони вже достатньо знають про безпечну поведінку в Інтернеті, тому подальша освіта не потрібна. Однак інтерв'ю також показало, що учасникам бракує знань у деяких сферах. Наприклад, під час виявлення фішингових електронних листів і веб-сайтів учасники визначили конкретні аспекти, які можна перевірити на законність, але кількість згаданих аспектів була неповною. Їм явно бракує знань про кроки, важливі для виявлення фішингових атак. Один учасник сказав, що він мав інтуїцію щодо безпеки веб-сайту та не знав, як правильно оцінити веб-сайт.

Інші були більш обізнаними, наприклад перевіряли ціни в онлайн-магазинах, щоб побачити, чи суттєво вони відрізняються від цін конкурентів, а також досліджували рейтинги, показники безпеки та веб-адреси.

Позитивним аспектом вважаю за потрібне вказати, що основні приклади небезпечної поведінки в інтернеті учнів не були виявлені. На мою думку, потрібно вказати деякі з них, задля створення власних рекомендацій для учнів навчальних закладів.

Небезпечна поведінка учнів навчальних закладів стосовно кібергігієни може включати наступні аспекти:

1. Спам та флуд: Учні можуть бути втягнуті у небезпечну поведінку, таку як надсилання спаму (небажаних повідомлень) або флуд (надмірних повідомлень), які можуть перебивати нормальну роботу учнів та заважати їм вивчати та спілкуватися в Інтернеті.

2. Розповсюдження небезпечної інформації: Учні можуть свідомо або ненавмисно розповсюджувати небезпечну або неправдиву інформацію в Інтернеті. Це може створювати паніку, спричиняти негативні наслідки для інших учнів або навіть поширювати шкідливі стереотипи.

3. Зловживання особистою інформацією: Учні можуть неконтрольовано розголошувати свою особисту інформацію в Інтернеті, таку як повне ім'я, адреса,

номери телефонів чи інші приватні дані. Це може призвести до небезпеки для їхньої особистої безпеки та може бути використано кіберзлочинцями.

4. Завантаження шкідливого вмісту: Учні можуть бути схильними до завантаження шкідливого вмісту, такого як насильство, порнографія або наркотики. Це може мати шкідливий вплив на їхнє психічне та емоційне здоров'я, а також порушити законодавство про дитячу безпеку в Інтернеті.

5. Психологічний тиск та маніпуляція: Деякі учні можуть використовувати кіберпростір для здійснення психологічного тиску, маніпуляцій або шантажу над іншими учнями. Це може призвести до стресу, тривоги та погіршення психічного здоров'я постраждалих.

6. Віруси та зловмисний код: Учні можуть недбало завантажувати файли або програми з ненадійних джерел, що може призвести до зараження комп'ютерів, планшетів або смартфонів вірусами та зловмисним кодом. Це може вплинути на пристрої, втрату даних та навіть використання їх для злочинних цілей.

7. Надмірне використання соціальних мереж: Деякі учні можуть проводити надмірно багато часу в соціальних мережах, що може вплинути на їх соціальні зв'язки, фізичне здоров'я та навчальні досягнення. Це може стати причиною ізольованості та зниження концентрації на навчанні.

8. Недоцільне використання особистих даних: Учні можуть недостатньо усвідомлювати значення приватності та небезпеки розголошення особистих даних. Вони можуть ділитися конфіденційною інформацією, такою як паролі, адреси електронної пошти, номери телефонів, з ненадійними джерелами або незнайомими людьми, що може призвести до зловживання цими даними.

9. Несанкціонований доступ до інформації: Учні можуть намагатись увійти до облікових записів інших учнів або вчителів, зламати паролі або отримати несанкціонований доступ до конфіденційної інформації. Це може включати доступ до особистих даних, оцінок, екзаменаційних завдань або інших конфіденційних матеріалів. Таке незаконне вторгнення в приватну сферу може мати серйозні наслідки для постраждалих осіб і порушувати довіру в навчальному середовищі.[13]

Ці небезпечні форми поведінки в кіберпросторі можуть мати серйозні наслідки для учнів, їхнього навчання та психологічного благополуччя. Важливо, щоб навчальні заклади та батьки спільно працювали над попередженням цих негативних явищ та надавали учням необхідні знання та навички кібербезпеки для безпечного та відповідального користування Інтернетом.

3.3 Сильні сторони та обмеження

Анкетування учнів навчальних закладів стосовно кібергігієни має свої сильні сторони та обмеження. Давайте розглянемо їх:

Сильні сторони анкетування:

1. Отримання відповідей від широкої аудиторії: Анкетування дає можливість зібрати думки та досвід різних учнів з різних класів та рівнів. Це дозволяє отримати репрезентативну картину стосовно їхньої кібергігієни.

2. Анонімність та конфіденційність: Анкетування може бути анонімним, що дає учням можливість відкрито висловити свої думки та досвід без страху перед негативними наслідками. Це сприяє більшій чесності та точності відповідей.

3. Швидкість та ефективність: Анкетування може бути проведене швидко та ефективно, особливо якщо використовуються електронні форми анкет. Це дозволяє отримати велику кількість відповідей за короткий час.

4. Масштабованість: Анкетування може бути проведене на велику кількість учнів і в різних навчальних закладах. Це дозволяє отримати широку географічну та соціальну репрезентативність результатів.

5. Стандартизація: Анкети можуть містити стандартизовані запитання, що дозволяє отримати порівняльну інформацію між учнями та групами. Це допомагає виявити загальні тенденції та патерни стосовно кібергігієни.

Обмеження анкетування:

1. Обмежена глибина розуміння: Анкетування може забезпечити лише обмежену кількість інформації про ставлення учнів до кібергігієни. Воно не

дозволяє дослідити в деталях їхні дії та мотивації, а також не надає можливості пояснити відповіді або задати додаткові запитання.

2. Недостатня об'єктивність: Учні можуть надавати неправдиві або необ'єктивні відповіді через бажання виглядати кращими або на зворотному боці - навмисно занижувати свою кібергігієну.

3. Вплив соціального бажання: Учні можуть відповідати так, як вони думають, що очікується від них або відповідно до соціальних норм, не відображаючи свої справжні переконання чи дії.

4. Обмежений контекст: Анкетування не враховує унікальні особливості кожного учня, його життєвий контекст та індивідуальні обставини, які можуть впливати на його кібергігієну.

5. Суб'єктивність відповідей: Учні можуть розуміти запитання по-різному та надавати суб'єктивні відповіді, що може призвести до спотворення результатів. Наприклад, один учень може вважати певну дію небезпечною, тоді як інший - ні.

6. Брак контролю: Анкетування не забезпечує прямого контролю над учнями та їхніми відповідями. Це може призводити до недостовірної інформації або пропуску важливих деталей.

7. Обмежена глибина аналізу: Анкетування не завжди дозволяє детально розібратися в причинах та контексті поведінки учнів в кіберпросторі. Для цього можуть знадобитися додаткові методи дослідження, які дозволять розширити розуміння ситуації.

Загалом, анкетування учнів є корисним інструментом для збору інформації про їхнє ставлення та поведінку в кіберпросторі. Проте, для отримання більш глибокого розуміння потрібно комбінувати його з іншими методами дослідження та враховувати обмеження, які випливають з його суб'єктивності та обмеженої глибини аналізу.

Це дослідження має деякі обмеження з вище перелічених. Невеликий розмір вибірки та обмежена кількість шкіл-учасниць можуть обмежити можливість узагальнення. Крім того, той факт, що інтерв’ю проводилися лише в одній школі, може негативно вплинути на узагальненість дослідження.

Іншим потенційним обмеженням є те, що опитувальник, який використовувався для цього дослідження, містить 16 пунктів, тоді як валідований опитувальник щодо обізнаності з інформаційною безпекою, який використовувався для розробки нашої анкети, містить 21 пункт для параметра поведінки. Можна стверджувати, що скорочена версія валідованої анкети не дає цілісної картини поведінки щодо інформаційної безпеки.

Однак скорочення анкети було важливим, оскільки не всі оригінальні запитання були актуальними для учнів початкової та старшої школи. У підсумку залишилося 14 релевантних пунктів, а ще 2 були додані на основі іншого опитування, щоб уникнути фішингових загроз. Значення елемента може змінитися, оскільки він перекладено та представлено іншим способом. Були проведені тести на валідність, щоб переконатися, що дослідження не були скомпрометовані. Такі елементи, як «безпечні паролі» та «регулярно перевіряйте налаштування безпеки», відкриті для тлумачення та повинні бути більш чітко визначені в майбутніх дослідженнях. Поточне формулювання пунктів взято з оригінальної валідованої анкети. Однак це формулювання має недоліки в дослідженнях і залишає більше місця для поганої самооцінки.

Усі респонденти заповнили опитування онлайн, щоб уникнути помилок копіювання. Щоб оцінити якість даних, було перевірено відсутність відповіді на вміст даних. Анкетування та групові інтерв'ю проводилися анонімно, щоб студенти могли чесно відповідати, не замислюючись про наслідки своїх відповідей. Крім того, анонімність зменшує можливість упередженості.

3.4 Майбутні дослідження

Бажано повторити поточне дослідження з більшим розміром вибірки та виконати його в багатонаціональному контексті. Більш детальне дослідження термінів в анкеті, які залишають простір для тлумачення, як-от використання «надійних паролів» і «регулярна перевірка налаштувань безпеки», може виявити важливі недоліки поведінки. Результати такого більш детального дослідження

можуть бути важливими для адекватного майбутнього дизайну навчального плану. Розвиваючи роботу Falkner et al. (2019), який порівнював навчальні програми, що використовуються в різних країнах, і на основі опублікованих навчальних програм K-12 можна розробити реальну міжнародну базову навчальну програму для дітей, яка буде адаптована для використання в різних культурах і країнах.[5] Крім того, було б цікаво дослідити, чому розширення існуючих навчальних програм було таким повільним. Опитування можна поширити на студентів вищих навчальних закладів, щоб дізнатися, чи стане кібербезпека у центрі уваги після закінчення середньої школи. Це пов’язано з тим, що деякі студенти ось-ось почнуть шукати роботу, і необхідно бути повністю готовим до можливості кібератак. Вивчення поведінки шкільних вчителів щодо кібербезпеки дає змогу краще зрозуміти поточні моделі поведінки.

Тема кібергігієни учнів навчальних закладів є досить розгалуженою. Існує безліч можливостей для майбутніх досліджень в цій галузі. Можна навести ще кілька ідей для такого роду досліджень:

1. Вивчення рівня обізнаності учнів щодо кібербезпеки: Дослідження можуть спрямовуватись на виявлення знань, умінь та свідомості учнів про основні принципи кібербезпеки. Можна дослідити, наскільки вони розуміють загрози, які стикаються в Інтернеті, та їхню готовність дотримуватися безпечних практик.

2. Аналіз небезпечної поведінки в мережі: Дослідження можуть вивчати типові небезпечні дії учнів в кіберпросторі. Це може включати розгляд ризикованого використання соціальних мереж, небажаного контенту, кібербулінгу, відсутності обережності щодо надання особистої інформації та інших проблем.

3. Ефективність освітніх програм з кібербезпеки: Дослідження можуть оцінювати ефективність різних освітніх програм, спрямованих на навчання учнів кібергігієні. Це дозволить з'ясувати, які підходи та методи найбільш успішні в підвищенні рівня кібербезпеки серед учнів.

4. Вивчення позитивного впливу батьківської участі: Дослідження можуть досліджувати вплив батьківської участі та контролю на кібергігієну учнів. Можна вивчити, наскільки батьківський нагляд та взаємодія сприяють безпеці в Інтернеті.

5. Розвиток інструментів та ресурсів: Дослідники можуть працювати над розробкою нових інструментів та ресурсів для покращення кібергігієни учнів. Це можуть бути мобільні додатки, освітні матеріали, веб-сайти або навіть віртуальні середовища для навчання учнів безпечному поводженню в Інтернеті.

6. Вплив соціальних мереж на психологічне благополуччя учнів: Дослідження можуть досліджувати, як використання соціальних мереж впливає на емоційний стан, самопочуття та самооцінку учнів. Це може включати аналіз зв'язку між використанням соціальних мереж та симптомами депресії, тривожності або низької самооцінки.

7. Вивчення взаємодії між учнями в кіберпросторі: Дослідники можуть аналізувати способи взаємодії між учнями у віртуальних середовищах, таких як форуми, чати або онлайн-ігри. Вивчення взаємодії та комунікації може допомогти виявити позитивні та негативні аспекти цього спілкування.

8. Розвиток навичок критичного мислення та медіаграмотності: Дослідження можуть спрямовуватись на розуміння та підвищення навичок критичного мислення учнів щодо інформації, яку вони зустрічають в кіберпросторі. Медіаграмотність може стати значущим аспектом для розробки програм та підходів, спрямованих на формування в учнів критичного ставлення до отриманої інформації та вміння розпізнавати фейкові новини.

9. Вивчення етичних аспектів використання технологій: Дослідники можуть проводити дослідження щодо етичних питань, пов'язаних з використанням технологій у навчальних закладах, наприклад, збереженням приватності, копіюванням та плагіатом, кібервикраденням тощо. Розуміння цих етичних аспектів може допомогти розробити ефективні політики та навчальні програми.[8]

Це лише кілька можливих напрямків досліджень. Тема кібергігієни учнів навчальних закладів має потенціал для подальшого вивчення та розвитку, спрямованого на підвищення безпеки та добробуту учнів у кіберпросторі.

Зважаючи на постійний розвиток технологій та зміну кіберпростору, не буде сюрпризом виникнення безлічі інших цікавих аспектів, які можна досліджувати в галузі кібергігієни учнів навчальних закладів в майбутньому.

До речі, варто зазначити, що Україна зробила певні зрушення на сьогоднішній день в галузі кібергігієни в цілому. Вже під час написання даної роботи з’явилось повідомлення і відбувся запуск освітнього серіалу «Основи кібергігієни. Як держслужбовцям захиститися від хакерських атак» на порталі «Дія» (Рисунок 3.1).[17] Даний серіал включає короткі ролики по 4-7 хвилин про різні види небезпек таких як: неправдиві повідомлення, соціальна інженерія, шкідливе програмне забезпечення та інші (Рисунок 3.2). Після закінчення курсу є можливість пройти фінальний іспит по викладеному в курсі матеріалу та перевірити рівень його засвоєння даного матеріалу і набуті навички в ході навчання.

Звісно, це невеликий крок для такої об’ємної теми як кібергігієна, але важливо, що початок розвитку вмінь доволі великої групи осіб як держслужбовці, зможе потягнути за собою хороші наслідки в галузі кібербезпеки в цілому і збільшити рівень обізнаності населення і його перехід до більш сучасної форми існування.

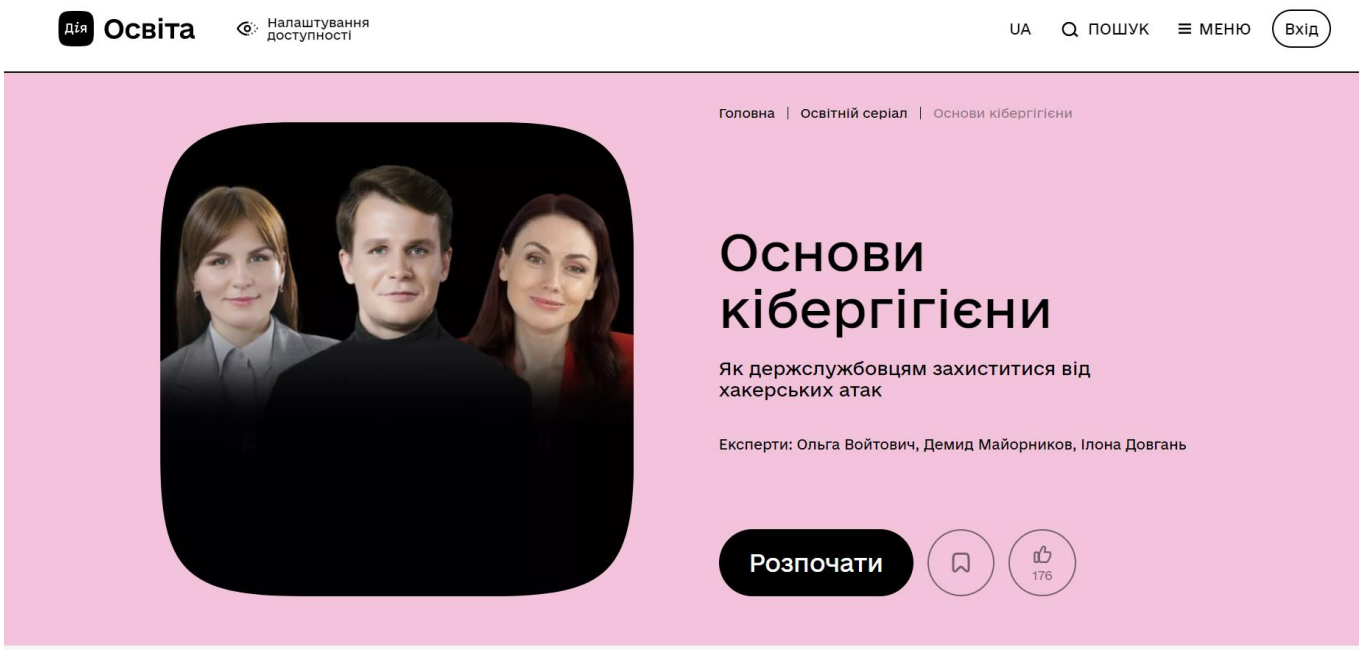

Рисунок 3.1 - Основи кібергігієни на сайті «Дія»

Рисунок 3.2 - Програма курсу на сайті «Дія»

3.5 Рекомендації для учнів щодо кібергігієни

Забезпечення кібергігієни учнів шкіл є вкрай важливим завданням у сучасному цифровому світі. Відповідне використання інтернет-ресурсів та електронних пристроїв може надати безліч можливостей для навчання та особистого розвитку, але також створює ризики з приводу приватності, кібербулінгу, крадіжки особистої інформації та інших кіберзагроз.

Отже, нижче наведено декілька рекомендацій щодо процедур кібергігієни для учнів шкіл:

1. Забезпечення безпеки паролів: Учні повинні використовувати міцні паролі для своїх облікових записів та регулярно їх змінювати. Пароль повинен бути унікальним для кожного облікового запису і складатися з комбінації букв, цифр та символів.

2. Розумне використання соціальних мереж: Учні повинні бути обізнані з наслідками того, яку інформацію вони публікують в соціальних мережах. Важливо регулярно переглядати налаштування приватності та обмежувати доступ до особистої інформації.

3. Запобігання кібербулінгу: Учні повинні бути свідомі про шкідливі наслідки кібербулінгу та поводитись в Інтернеті з повагою до інших. Важливо повідомляти про будь-які випадки кібербулінгу вчителям або шкільним адміністраторам.

4. Розумне завантаження та використання контенту: Учні повинні розуміти, що завантажування незаконного або шкідливого контенту може мати серйозні наслідки.

5. Освіта щодо кібербезпеки: Школи повинні включати навчання з кібербезпеки до своїх програм навчання. Учні повинні бути ознайомлені з основними поняттями кібербезпеки, такими як фішинг, віруси, зловмисні програми тощо, і знати, як реагувати на них.

6. Встановлення фільтрів та обмежень: Школи та батьки повинні встановлювати фільтри та обмеження на веб-сайти та додатки, які використовують учні. Це допоможе уникнути доступу до небажаного або небезпечного контенту.

7. Регулярне оновлення програмного забезпечення: Учні повинні регулярно оновлювати програмне забезпечення на своїх пристроях, включаючи операційні системи та антивірусні програми. Це допоможе уникнути вразливостей, які можуть бути використані зловмисниками.

8. Свідоме використання особистої інформації: Учні повинні розуміти, яку особисту інформацію можна розголошувати в Інтернеті. Важливо вчити їх уникати розголошення конфіденційної інформації, такої як адреси, номери телефонів чи інформація про родину.

9. Захист від шкідливих програм: Учні повинні бути навчені встановлювати та оновлювати антивірусне програмне забезпечення на своїх пристроях. Вони також повинні бути попереджені про ризики завантаження невідомих файлів або програм.

10. Виявлення і повідомлення про кіберзагрози: Учні повинні бути здатними розпізнавати ознаки кіберзагроз, таких як фішингові повідомлення або підозрілі веб-

сайти. Важливо навчати їх ефективно повідомляти про такі випадки вчителям або шкільним адміністраторам.

11. Створення позитивного цифрового сліду: Учні повинні бути свідомими про своє онлайн-поведінку та її вплив на їх майбутнє. Важливо навчати їх створювати позитивний цифровий слід, проявляючи повагу до інших, уникати цифрової некоректності та розповсюдження шкідливого контенту.

12. Залучення батьків та вчителів: Важливо, щоб батьки та вчителі активно співпрацювали у створенні безпечного цифрового середовища для учнів. Це може включати проведення батьківських зборів, розповідь про кібербезпеку та спільне навчання учнів правильному використанню Інтернету та електронних пристроїв.

До рекомендацій можна також додати, що навчальному закладі як структурі бажано ввести засоби контролю для вирішення цих ризиків, щоб кіберсистема відповідала законодавству України, зокрема закону України про основні засади забезпечення кібербезпеки України[15], рішенню РНБО “Про Стратегію кібербезпеки України”[12], національним стандартам України, в тому числі ДСТУ ISO/IEC 27032:2012, і могла включаючи засоби контролю для:

- підготовки до атак, наприклад, шкідливих програм, окремих зловмисників або злочинних організацій в Інтернеті;

- виявлення та моніторингу атак;

- реагування на напади.

Оскільки Україна має проєвропейський курс, тому перехід на загальноєвропейські стандарти є лише питанням часу.[14] Тому поступовий перехід навчальних закладів зараз на єдині стандарти кібербезпеки дозволить систематизувати реагування на кіберінциденти і розробити єдині алгоритми дій в разі атак уже найближчим часом та покаже чи зможе українська система освіти адаптуватись до нових реалій.

Загальним принципом усіх цих рекомендацій є розвиток свідомого, відповідального та безпечного використання цифрових технологій серед учнів. Вчителі, батьки та шкільні адміністратори мають працювати разом, щоб забезпечити ефективну інформаційну освіту та практичні навички кібербезпеки для молоді.

Застосування процедур кібергігієни в школах створює безпечне і довірливе середовище для учнів, де вони можуть максимально використовувати цифрові ресурси для свого навчання та розвитку. Це не лише допоможе їм уникнути потенційних кіберзагроз, але й розвивати навички цифрової грамотності, критичного мислення та етичного поведінки в Інтернеті.

Зростання впевненості учнів у сфері кібербезпеки має значний вплив на їхню майбутню кар'єру та особисте життя. Розуміння кібергігієни та вміння застосовувати її принципи стануть важливими компетенціями, що допоможуть учням стати активними, впевненими та безпечними учасниками цифрового світу.

Вважаю, що реалізація процедур кібергігієни для учнів шкіл сприятиме створенню надійного та захищеного цифрового середовища, де молодь зможе іти в ногу з часом та не відчуватиме труднощів у навчанні і повсякденному житті.

Висновок до розділу 3

В результаті проведення анкетування учнів навчальних ми змогли розглянути і дослідити сильні сторони та обмеження методу анкетування, проаналізувати основні небезпеки учням навчальних закладів, можливі майбутні дослідження в даній галузі, сформовано рекомендації учням щодо кібергігієни.

Варто зазначити, що спектр майбутніх досліджень може бути значно більшим, адже галузь кібербезпеки змінюється щоденно, в зв'язку з виникненням нових загроз, ризиків, видів шахрайств в кіберпросторі. Проте сформовані рекомендації, сподіваюсь допоможуть в вирішенні ряду наявних проблем. Також з розвитком галузі вони можуть бути змінені і актуалізовані під нові виклики.

ВИСНОВКИ

Я рекомендую вивчати правила кібербезпеки на ранньому етапі базової шкільної освіти. Як самі учні зазначали в інтерв'ю, важливо, щоб учні, ймовірно, повторювали уроки, пов'язані з кібербезпекою, пізніше в початковій школі після того, як вони отримали свої перші шкільні пристрої (наприклад, ноутбуки та iPad). Потрібно звернути особливу увагу на виявлення фішингових електронних листів і фішингових веб-сайтів. Студенти повинні знати, що ризикована поведінка в Інтернеті може негативно вплинути на них та їхні організації. Приклад крадіжки особистих даних і його драматичний вплив на життя людини має бути представлений переконливо. Так само, як грамотність і математика, кібербезпека має бути частиною базової освіти. Можливо, якби кібербезпека була введена в програму навчання, навіть як підрозділ наявного предмету інформатика, це дозволило б знизити рівень кіберінцидентів та підвищити самосвідомість та самоаналіз учнів навчальних закладів. Слід розглянути можливість використання відомих навчальних програм, таких як PICSAR.

Результати цього дослідження надають попередні докази того, що учні початкової та старшої школи не можуть ефективно розвивати кібербезпечну поведінку в повному обсязі самостійно без допомоги викладачів. Але важливо зауважити, що потрібно ділитись своїми проблемами в кіберпросторі, бо це дозволить проаналізувати власні помилки, щоб не повторювати цього в майбутньому. Студенти повідомили про поведінку в кібербезпеці, пов'язану з електронною поштою, паролями, фішингом і фізичним блокуванням пристроїв, але багато студентів також розвинули надмірну самовпевненість і необачну поведінку в сферах користування Інтернетом і онлайн-повідомлень про інциденти. Учні виявили, що школи відіграють незначну роль у розвитку кібергігієни. Проте їхні поодинокі дії можуть зашкодити школі, як структурі в цілому. Учні набули поведінки в Інтернеті переважно завдяки досвіду, онлайн-класам, а також завдяки їхньому оточенню.

А завданням на майбутнє для суспільства вважаю, що кіберзагрози суб’єктам навчальних закладів швидше мають стати рідкістю, ніж сталою закономірністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The Global Information Technology Report 2016 URL: https://formatresearch.com/img/file/varie/2016/WEF_GITR_Full_Report.pdf

2. Teaching Cybersecurity: Introducing the Security Mindset Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 2 (SIGCSE 2022). (2022), p. 1195

3. ДСТУ ISO/IEC 27032:2012 «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 2018.01.01 URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128 (дата звернення: 10.06.2023).

4. Cyber security education: Why don't we do anything about it? ACM Inroads, 8 (4) (2017), p. 5, 10.

5. Перетворення комп'ютерної освіти K-12: принципи інформатики AP® ACM Inroads , 6 (4) (2015) , стор . 58–59

6. Навчання безпеки від фішингу: скромна пропозиція про серйозне переосмислення IEEE Security Privacy , 10 (2) (2012) , стор . 24–32

7. Cybersecurity behavior: A conceptual taxonomy O. Blazy, C.Y. Yeun (Eds.), Information security theory and practice, Springer International Publishing (2019), pp. 147-156

8. Кібергігієна. Кібербезпека. Безпека держави : матеріали наукових семінарів (Київ, 27 листопада 2020 р.) / відп. ред. А. М. Десятко. – Київ : Київ. нац. торг.-екон. ун-т, 2020. – 101 с.

9. Nikolic, B., Rueben, R. Cyber (2015) Hygiene practices for secure e-learning environments. International Journal of Information and Education Technology, 5(10), 777-782.

10. Kupreev, O., Gutnikov, A., & Kovaleva, E. (2020). Cybersecurity education in higher education institutions: A systematic literature review. Information, 11(9), p. 420.

11. Grant, K. J., Fodor, G. (2019). Cybersecurity awareness training: An analysis of current approaches and recommendations for improvement. International Journal of Cybersecurity Intelligence & Cybercrime, 2(1), 7-20. [Electronic journal].

12. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" Указ Президента №447/2021 від 14 травня 2021 року URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 27.03.2023).

13. Bart R. McDonough (2018). Cyber Smart. Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals, 5(10), 23-27.

14. Сліпченко Т. Кібербезпека як складова системи захисту національної безпеки: європейський досвід / Сліпченко Т. // Тернопільський національний економічний університет - Тернопіль, 2020.

15. Закон України Про основні засади забезпечення кібербезпеки України від 17.08.2022 URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

16. Veronica Rose (2021). Cyber Hygiene for Children. Raising Cyber Aware Children, p. 47-51

17. Сайт МЦТУ «Дія.Освіта». Курс Основи кібергігієни. «Як держслужбовцям захиститися від хакерських атак». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene

18. Greenfield P.M. Mind and Media: The Effects of Television, Video Games, and Computers. Cambridge Mass.: Harvard University Press, 2004. 232 p.

19. Richard Philips, Rayton R. Sianjina. Cyber Security for Educational Leaders. A Guide to Understanding and Implementing Technology Policies. Routledge, New York and London, 2013. 96 p.

20. Leslie F. Sikos, Paul Haskell-Dowland.Cybersecurity Teaching in Higher Education. Springer, School of Science Australia, 2023, p. 79-83

21. Jacob Willem Abraham Witsenboer, MSc, Klaas Sijtsma, MSc PhD, Fedde Scheele, MD PhD. Measuring cyber secure behavior of elementary and high school students in the Netherlands, 2022, 186 p., [Electronic journal] URL: https://www.sciencedirect.com/science/article/pii/S0360131522001075?ref=pdf_download&fr=RR-9&rr=7da66ab9b90b24c1

ДОДАТОК А
ОПИС І УЗАГАЛЬНЕНІ РЕЗУЛЬТАТИ ПРОВЕДЕНИХ ОПИТУВАНЬ СЕРЕД УЧНІВ

Опис	Результати
Розпізнавання фішингових електронних листів	Старшокласники можуть розпізнавати фішингові електронні листи краще, ніж учні початкової школи.
Розпізнавання фішингових веб-сайтів	Старшокласники можуть розпізнавати фішингові веб-сайти краще, ніж учні початкової школи.
Введення даних онлайн	Старшокласники недостатньо оцінюють безпеку веб-сайтів перед введенням інформації.
Налаштування конфіденційності в соціальних мережах	Старшокласники майже не перевіряють налаштування конфіденційності своїх акаунтів у соціальних мережах
Повідомлення про дивні ситуації	Учні початкової школи діляться цим із батьками, якщо вони відчувають щось дивне в Інтернеті. Старшокласники роблять це недостатньо.
Блокування мобільних пристроїв	Старшокласники залишають свій ноутбук/iPad/мобільний телефон зачиненими в класі. Учні початкової школи не блокують свої пристрої належним чином.
Завантаження файлів	Старшокласники завантажують усі потрібні файли на свої шкільні комп’ютери та відвідують будь-який веб-сайт, який їм заманеться.